HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400
APO AE 09131-0400

DIRECTIVE NUMBER 25-11

2 December 2002

SECURITY

Travel Briefing Requirements for Designated Personnel

1. **Purpose**. To prescribe polices and procedures requiring security briefings for all U.S. personnel possessing a security clearance and/or those indoctrinated for access to Sensitive Compartmented Information (SCI).

2. **Applicability**. This Directive applies to all HQ USEUCOM Directorates/Staff offices and activities internal and external to the Headquarters, not including component commands.

3. **Internal Control Systems**. This Directive contains internal control provisions and is subject to requirements of the internal management control program. For HQ USEUCOM and subordinate joint activities, the applicable internal control directive is ED 50-8, Internal Management Control Program.

4. **Suggested Improvements**. The proponent for this directive is the Intelligence Directorate, Security Support Office. Suggested improvements should be forward to HQ USEUCOM, Attn: ECJ2-SSO, Unit 30400, APO AE 09131-0400.

5. **References**.

a. DoD 5200.2-R, Personnel Security Program, January 1987 (U).

b. DoD S-5105.21-M-1, Sensitive Compartmented Information Administrative Security Manual, March 1995 (U).

c. Director of Central Intelligence Directive (DCID) 1/20P, Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI), 29 December 1991 (U).

d. CJCS Instruction 3231.01, Safeguarding the SIOP, dated 30 Nov 93 (U).

This Directive supersedes ED 25-11, dated 5 Feb 96.

6. **Explanation of Terms**.

a. ***Defensive Security Briefings***. Formal advisories that alert traveling personnel to the potential for harassment, exploitation, provocation, capture, or entrapment. These briefings, based on actual experience, include information on courses of action helpful in mitigating adverse security and personnel consequences, and advice of passive and active measures that personnel should take to avoid becoming targets or inadvertent victims as a consequence of hazardous travel.

b. ***Official Travel***. Travel performed at the direction of the U.S. Government.

c. ***Unofficial Travel***. Travel undertaken by an individual without official, fiscal or other obligations on the part of the U.S. Government.

d. ***Class I Personnel***. U.S. military, civilian and DOD contractor personnel indoctrinated for any level of access to Sensitive Compartmented Information (SCI).

e. ***Class II Personnel***. Persons other than those designated as Class 1 who possess a DOD security clearance and are considered by their directors or activity heads as vulnerable because of their broad knowledge of critical defense matters. Generally, this includes persons who are engaged in working with war plans, cover and deception, plans and polices, restricted data, Critical Nuclear Weapons Design Information (CNWDI), the Single Integrated Operational Plan -Extremely Sensitive Information (SIOP-ESI), Special Contingency Plans, similarly critical information or activities, and specifically those possessing a U.S. Top Secret clearance. This applies to U.S. military, civilian, and DOD contractor personnel.

f. ***Hazardous Travel***. Travel to, through, or within countries that pose a threat to Class I and II personnel. Hazardous travel includes:

(1) Travel to, through, or within:

(a) Combat zones

(b) Countries identified as medium or high risk by the States Department or DoD.

(c) Areas in which the threat to U.S. personnel from foreign intelligence services, terrorist or indigenous groups active in promoting insurgency, war, or civil unrest, where the physical safety and security of personnel and sensitive information cannot be reasonably ensured.

(2) Travel or visits to diplomatic or trade mission of counties identified as medium or high risk by the State Department or DoD.

(3) Travel on transportation carriers owned or controlled by a country identified as medium or high risk by the State Department or DoD.

7. **Responsibilities**.

a. The EJC2 Security Support Office (ECJ2-SSO) will:

(1) Maintain a master Roster of all Class I and Class II Personnel.

(2) Distribute State Department, DoD and other appropriate Agency warnings to Directorate or Activity Security Managers, subordinate SSOs, SCIF Custodians and Special Security Representatives.

(3) Maintain a master file of all Class II Personnel.

(4) Distribute State Department and other appropriate Agency warnings to Directorate or Activity Security Managers, as needed.

b. At HQ USEUCOM, Unit/Activity SCI Billet Managers will process the HQ USEUCOM Form 25-l1A-R and arrange for Defensive Security Briefings for Class I Personnel under their jurisdiction. Locations outside of HQ USEUCOM will coordinate directly with their managing SSO.

c. HQ USEUCOM Directorate/Unit Security Managers, or their designated appointee, will:

(1) Process the HQ USEUCOM Form 25-l1B-R and arrange for Defensive Security Briefing for Class II Personnel under their Jurisdiction.

(2) Ensure those personnel with access to other programs having travel restrictions or requiring special briefings/debriefings are referred to the appropriate program manager or administrator. This includes personnel in both classes I and II. Examples include, but are not limited to, those personnel read on to Special Access Programs (SAP) and/or SIOP-ESI or CNWDI.

8. **Policies and Procedures**. Persons granted access to SCI, or other sensitive information, incur a special security obligation, and with the exception of official travel, are discouraged from traveling to countries deemed hazardous by the state department or this command. All travelers must be alerted to the risks associated with hazardous travel. Failure to comply with the following provision may result in the withdrawal of access to SCI or other classified national defense information, and may be considered in determining whether future access is warranted.

a. Official Travel. Class I and II Personnel who plan travel to, through, or within countries deemed hazardous shall:

(1) In advance, submit an itinerary to their designated representative.

(2) Receive a Defensive Security Briefing.

(3) Report efforts by any individual, regardless of nationality, to obtain illegal or

unauthorized access to classified or sensitive unclassified information. Any suspected attempts to place cleared individuals in compromising situations, or any contract that suggests possible attempts at exploitation by intelligence services of another country, will also be reported. Do not report contacts over non-secure telephone lines.

(a) If possible, while traveling, report unusual incidents to the nearest US Consulate.

(b) Upon return to your duty station, report the unusual incident to the nearest Counterintelligence office of record. At HQ USEUCOM, this is either the local USAF Office of Special Investigations (OSI), if a member of the USAF, or the 527th USA Military Intelligence Battalion, for other service members, civilians and contractors.

b. Unofficial Travel.

(1) Class I Personnel who plan to travel to, through, or within countries deemed hazardous shall comply with all the aforementioned requirements for official travel.

(2) Class II Personnel are required to comply only with the provisions of paragraph 8.a.(3) above. However, those Class II personnel having SIOP-ESI access must comply with all provisions of paragraph 8.a above.

c. Frequent Official Travel. Class 1 and II Personnel performing official travel on a continuous basis to hazardous areas may, rather than submitting multiple itineraries, submit a Memorandum For Record stating the location and the anticipated frequency of the travel. This memorandum will be submitted to the designated representative. In lieu of a briefing for each projected travel, the designated representative will arrange a Defensive Security Briefing at least semi-annually.

FOR THE COMMANDER:

OFFICIAL:

JOHN B. SYLVESTER
Lieutenant General, USA
Chief of Staff

RICKEY K. WILLIAMS
LTC, USA
Adjutant General

DISTRIBUTION:
P

APPENDIXES: